(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－158654
（Ｐ２００２－１５８６５４Ａ）
(43)公開日　平成14年５月31日(2002.5.31)

| (51)Int.Cl.[7] | 識別記号 | Ｆ Ｉ | | テーマコード（参考） |
|---|---|---|---|---|
| H04L 9/16 | | H04L 9/00 | 643 | 5C064 |
| 9/08 | | | 601 Z | 5J104 |
| H04N 7/167 | | | 601 E | |
| | | H04N 7/167 | Z | |

審査請求　未請求　請求項の数14　ＯＬ　（全23頁）

(21)出願番号　特願2000－351510（Ｐ2000－351510）

(22)出願日　平成12年11月17日(2000.11.17)

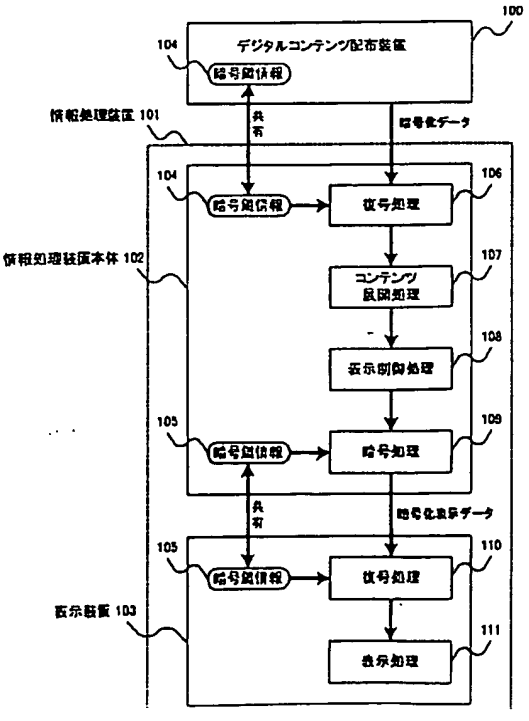
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　大和田　徹
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　北原　潤
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100084032
弁理士　三品　岩男　（外１名）

最終頁に続く

(54)【発明の名称】情報処理装置、表示装置、デジタルコンテンツ配布システム、および、デジタルコンテンツ配布・出力方法

(57)【要約】
【課題】デジタルコンテンツの権利を保護しつつ、ユーザの視聴覚欲求を刺激する形でのデジタルコンテンツの最終出力を可能とする。
【解決手段】情報処理装置本体１０２が、表示装置１０３と共有する暗号鍵情報１０５を用いて暗号化したデジタルコンテンツ（表示データ）を、表示装置１０３に転送し、表示装置１０３が、情報処理装置本体１０２から転送される表示データに対して、暗号鍵情報１０５を用いてを用いて復号処理を施すようにしている。ここで、情報処理装置本体１０２から表示装置１０３に転送される表示データは、例えば、数ライン分おきに、数ライン分の表示データずつが暗号化されるなど、一部分のみが暗号化されたものである。

図１



1

【特許請求の範囲】
【請求項1】処理装置および出力装置を少なくとも備えた情報処理装置において、
上記処理装置は、
デジタルコンテンツに対して、上記出力装置と共有する暗号鍵情報を用いて暗号処理を施す暗号処理手段と、
暗号化されたデジタルコンテンツを上記出力装置に転送する転送手段とを備え、
上記出力装置は、
上記処理装置から転送されるデジタルコンテンツを入力する入力手段と、
入力したデジタルコンテンツに対して、上記処理装置と共有する暗号鍵情報を用いて復号処理を施す復号処理手段と、
暗号化部分を復号後のデジタルコンテンツを出力する出力手段とを備えたことを特徴とする情報処理装置。
【請求項2】処理装置および出力装置を少なくとも備えた情報処理装置において、
上記処理装置は、
デジタルコンテンツの一部分に対して、上記出力装置と共有する暗号鍵情報を用いて暗号処理を施す暗号処理手段と、
一部分が暗号化されたデジタルコンテンツを上記出力装置に転送する転送手段とを備え、
上記出力装置は、
上記処理装置から転送されるデジタルコンテンツを入力する入力手段と、
入力したデジタルコンテンツに対して、上記処理装置と共有する暗号鍵情報を用いて復号処理を施す復号処理手段と、
暗号化部分を復号後のデジタルコンテンツを出力する出力手段とを備えたことを特徴とする情報処理装置。
【請求項3】処理装置および出力装置を少なくとも備えた情報処理装置において、
上記処理装置は、
暗号化されたデジタルコンテンツを入力する入力手段と、
入力したデジタルコンテンツに対して、該デジタルコンテンツを復号するための暗号鍵情報を用いて復号処理を施す復号処理手段と、
復号後のデジタルコンテンツの一部分に対して、上記出力装置と共有する暗号鍵情報を用いて暗号処理を施す暗号処理手段と、
暗号化されたデジタルコンテンツを上記出力装置に転送する転送手段とを備え、
上記出力装置は、
上記処理装置から転送されるデジタルコンテンツを入力する入力手段と、

2

段と、
暗号化部分を復号後のデジタルコンテンツを出力する出力手段とを備えたことを特徴とする情報処理装置。
【請求項4】暗号化されたデジタルコンテンツを入力する入力手段と、
入力したデジタルコンテンツに対して、該デジタルコンテンツを復号するための暗号鍵情報を用いて復号処理を施す復号処理手段と、
復号後のデジタルコンテンツの一部分に対して、該デジタルコンテンツの出力先の出力装置と共有する暗号鍵情報を用いて暗号処理を施す暗号処理手段と、
一部分が暗号化されたデジタルコンテンツを上記出力装置に転送する転送手段とを備えたことを特徴とする情報処理装置。
【請求項5】請求項3または4記載の情報処理装置であって、
上記入力手段が入力するデジタルコンテンツは、
平文時のデジタルコンテンツのフォーマッティング単位を1単位とし、これらの単位の一部の単位が暗号化対象となるようにして暗号化されていることを特徴とする情報処理装置。
【請求項6】請求項2，3，4または5記載の情報処理装置であって、
上記暗号処理手段は、
平文時のデジタルコンテンツのフォーマッティング単位を1単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すことを特徴とする情報処理装置。
【請求項7】請求項2，3，4または5記載の情報処理装置であって、
上記出力装置が音声再生装置である場合に、
上記暗号処理手段は、
上記音声再生装置に出力する音声データについて、複数サンプル分の音声データを1単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すことを特徴とする情報処理装置。
【請求項8】請求項2，3，4または5記載の情報処理装置であって、
上記出力装置が表示装置である場合に、
上記暗号処理手段は、
上記表示装置に出力する表示データのライン方向に、複数ライン分の表示データを1単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すか、または、上記表示装置に出力する表示データのカラム方向に、複数カラム分の表示データを1単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すことを特徴とする情報処理装置。
【請求項9】請求項2，3，4または5記載の情報処理

上記暗号処理手段は、
上記表示装置に出力する表示データの１画素分のデータを１単位とし、これらの単位の一部または全部について、各々、その一部分を暗号処理の処理対象として、暗号処理を施すことを特徴とする情報処理装置。
【請求項１０】暗号化された表示データを入力する入力手段と、
入力した表示データに対して、該表示データの転送元の情報処理装置と共有する暗号鍵情報を用いて復号処理を施す復号処理手段と、
暗号化部分を復号後の表示データを表示する表示手段とを備えたことを特徴とする表示装置。
【請求項１１】請求項１０記載の表示装置であって、
上記入力手段が入力するデジタルコンテンツは、
平文時の表示データのライン方向に、複数ライン分の表示データを１単位とし、これらの単位の一部の単位が暗号処理の処理対象となるようにして暗号化されているか、または、平文時の表示データのカラム方向に、複数カラム分の表示データを１単位とし、これらの単位の一部の単位が暗号処理の処理対象となるようにして暗号化されていることを特徴とする表示装置。
【請求項１２】請求項１０記載の情報処理装置であって、
上記入力手段が入力するデジタルコンテンツは、
平文時の表示データの１画素分のデータを１単位とし、これらの単位の一部または全部について、各々、その一部分が暗号処理の処理対象となるようにして暗号化されていることを特徴とする表示装置。
【請求項１３】デジタルコンテンツを配布するデジタルコンテンツ配布装置と、デジタルコンテンツ配布装置から配布されるデジタルコンテンツを出力装置に転送して出力する情報処理装置とを備えたデジタルコンテンツ配布システムにおいて、
上記デジタルコンテンツ配布装置は、
上記情報処理装置と共有する第１の暗号鍵情報を用いて一部分が暗号化されたデジタルコンテンツを蓄積している蓄積手段と、
蓄積しているデジタルコンテンツを上記情報処理装置に配布する配布手段とを備え、
上記情報処理装置は、
上記デジタルコンテンツ配布装置から配布されるデジタルコンテンツを入力する入力手段と、
入力したデジタルコンテンツ中の暗号化部分に対して、上記第１の暗号鍵情報を用いて復号処理を施す復号処理手段と、
暗号化部分を復号後のデジタルコンテンツの一部分に対して、上記出力装置と共有する第２の暗号鍵情報を用いて暗号処理を施す暗号処理手段と、
暗号化されたデジタルコンテンツを上記出力装置に転送
上記出力装置は、
上記情報処理装置から転送されるデジタルコンテンツを入力する入力手段と、
入力したデジタルコンテンツ中の暗号化部分に対して、上記第２の暗号鍵情報を用いて復号処理を施す復号処理手段と、
暗号化部分を復号後のデジタルコンテンツを出力する出力手段とを備え、
上記デジタルコンテンツ配布装置の暗号処理手段、および、上記情報処理装置の暗号処理手段は、
平文時のデジタルコンテンツのフォーマッティング単位を１単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すことを特徴とするデジタルコンテンツ配布システム。
【請求項１４】デジタルコンテンツを配布するデジタルコンテンツ配布装置と、デジタルコンテンツ配布装置から配布されるデジタルコンテンツを出力装置に転送して出力する情報処理装置とを備えたデジタルコンテンツ配布システムにおいて、上記デジタルコンテンツ配布装置から上記情報処理装置へデジタルコンテンツを配布して上記出力装置で出力する方法であって、
上記デジタルコンテンツ配布装置が、上記情報処理装置と共有する第１の暗号鍵情報を用いて一部分が暗号化されたデジタルコンテンツを、上記情報処理装置に配布し、
上記情報処理装置が、上記デジタルコンテンツ配布装置から配布されるデジタルコンテンツ中の暗号化部分に対して、上記第１の暗号鍵情報を用いて復号処理を施し、
暗号化部分を復号後のデジタルコンテンツの一部分に対して、上記出力装置と共有する第２の暗号鍵情報を用いて暗号処理を施してから、暗号化後のデジタルコンテンツを上記出力装置に転送し、
上記出力装置が、上記情報処理装置から転送されるデジタルコンテンツ中の暗号化部分に対して、上記第２の暗号鍵情報を用いて復号処理を施し、暗号化部分を復号後のデジタルコンテンツのを出力し、
上記デジタルコンテンツ配布装置が配布するデジタルコンテンツ、および、上記情報処理装置が転送するデジタルコンテンツは、
平文時のデジタルコンテンツのフォーマッティング単位を１単位とし、これらの単位中の一部の単位が暗号化対象となるようにして暗号化されていることを特徴とするデジタルコンテンツ配布・出力方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、著作権保護が必要なデジタルコンテンツを扱う技術に関し、特に、複製による不正使用を防ぎ、かつ、正当な使用権利を持たないユーザの視聴覚欲求を刺激する形での利用を可能としな

装置で出力する方法に関する。

【0002】

【従来の技術】近年、映像や音声などの高付加価値な情報をデジタル形式で配布する要求が高まっており、デジタルコンテンツの著作権保護を図るために、不正コピーの防止が重要視されてきている。すなわち、デジタルコンテンツは、容易にコピーできる上、コピーしても品質が劣化しないので、既に不正コピーによる著作権の侵害等の弊害が生じてきている。

【0003】コピー防止手段の1つとしては、一般に、デジタルコンテンツの暗号化が用いられており、正当な暗号鍵情報を入手したユーザのみが、暗号化されたデジタルコンテンツを復号し、その中身を確かめることができるようにしている。

【0004】

【発明が解決しようとする課題】しかしながら、デジタルコンテンツを単純に暗号化した場合、暗号化されたデジタルコンテンツは、正当な暗号鍵情報がないと全く視聴することができなくなってしまう。

【0005】これは、デジタルコンテンツが何らかのフォーマットに従ってフォーマッティングされているにも関わらず、フォーマットを無視した単純な暗号化が行われることにより、デジタルコンテンツのデータ構造が破壊されてしまい、デジタルコンテンツを再生するソフトウェアやハードウェアがデータ構造を全く解釈できなくなるからである。

【0006】そこで、ユーザは、デジタルコンテンツを購入するなどして、正当な暗号鍵情報を入手しない限り、その中身を確かめることができず、ユーザにとってはデジタルコンテンツ購入の敷居が高くなってしまう。

【0007】このような問題を解決するためには、デジタルコンテンツの権利保護を大前提にしつつも、ユーザの視聴覚欲求を刺激する形でデジタルコンテンツを配布するようにすることが好ましい。

【0008】また、従来、デジタルコンテンツの暗号化は、ユーザの情報処理装置に到達するまでの経路についてのみ行われており、情報処理装置において、表示装置などの最終出力装置へ出力する際の経路については、暗号化による著作権保護の対象とはなっていない。

【0009】近年、従来のCRT (Cathode-Ray Tube) 表示装置のようなアナログ入力の最終出力装置に代わり、液晶表示装置のようなデジタル入力の最終出力装置が一般化しつつあることから、このような最終出力装置へ出力する際の経路で、デジタルコンテンツの不正コピーが行われる恐れがある。

【0010】そこで、本発明の目的は、情報処理装置において、デジタルコンテンツを最終的に出力する際の経路での不正コピーを防止することを可能にすることにあり、デジタルコンテンツの権利を保護すると共に、ユーザの視聴覚欲求を刺激することにより、デジタル時コンテンツの配布または販売を促進することを可能にすることにある。

【0012】

【課題を解決するための手段】上記目的を達成するために、本発明は、処理装置および出力装置を少なくとも備えた情報処理装置において、上記処理装置が、上記出力装置と共有する暗号鍵情報を用いて暗号化したデジタルコンテンツを、上記上記出力装置に転送し、上記出力装置が、上記処理装置から転送されるデジタルコンテンツに対して、上記暗号鍵情報を用いて復号処理を施すようにしている。

【0013】そして、特に、本発明では、もう1つの目的を達成するために、上記処理装置から上記出力装置に転送されるデジタルコンテンツが、平文時のデジタルコンテンツのフォーマッティング単位を1単位とし、これらの単位の一部の単位が暗号化対象となるようにして暗号化されたものであるようにしている。

【0014】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。

【0015】図1は、本実施形態に係るデジタルコンテンツ配布システムの概略構成図である。

【0016】図中、100はデジタルコンテンツ配布装置、101は情報処理装置、102は情報処理装置本体、103は表示装置である。

【0017】本実施形態に係るデジタルコンテンツ配布システムは、デジタルコンテンツ配布装置100によってデジタルデータとして配布される高付加価値コンテンツの権利保護を大前提としている。すなわち、本実施形態に係るデジタルコンテンツ配布システムは、デジタルコンテンツ配布装置100と情報処理装置本体102との間を転送されるデジタルコンテンツ（配布データ）、および、情報処理装置本体102と表示装置103との間を転送されるデジタルコンテンツ（表示データ）が、各々、デジタルデータであるようなものを対象にしており、これらを暗号化することで保護を図っている。

【0018】そして、本実施形態に係るデジタルコンテンツ配布システムは、ユーザの視聴覚欲求を刺激する形でデジタルコンテンツを配布可能とすることを目的としている。すなわち、本実施形態に係るデジタルコンテンツ配布システムは、暗号化されたデジタルコンテンツで、ユーザの視聴覚要求を刺激することを可能とするものである。

【0019】具体的には、デジタルコンテンツ配布装置100と情報処理装置本体102との間を転送されるデジタルコンテンツは、例えば、JPEG (Joint Photog

ーマッティングされたデジタルデータが、例えば、ＤＥＳ（Data Encryption Standard）などの、予め決められた暗号方式で暗号化された暗号化データである。

【００２０】ここで、デジタルコンテンツ配布装置１００は、ネットワークを経由してデジタルコンテンツを配布するネットワーク装置であっても、例えば、光ディスク媒体や磁気ディスク媒体などの、デジタルコンテンツが記録された記録媒体であってもよい。

【００２１】すなわち、デジタルコンテンツ配布装置１００によって配布されるデジタルコンテンツは、デジタルコンテンツ配布装置１００から配布される時点で暗号化されていればよく、暗号処理を施すのがデジタルコンテンツ配布装置１００でなくてもよい。

【００２２】さて、図１に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、デジタルコンテンツ配布装置１００および情報処理装置本体１０２は、何らかの方法によって、デジタルコンテンツ（配布データ）を暗号化／復号化するための暗号鍵情報１０４を共有する機能を有している。

【００２３】暗号鍵情報１０４を共有する方法については、様々な方法が公知技術となっており、どのような方法を採用してもよい。

【００２４】例えば、デジタルコンテンツの暗号化に用いられた暗号鍵情報１０４を管理しているネットワーク装置から、情報処理装置本体１０２が暗号鍵情報１０４を入手するという方法が挙げられる。このとき、ネットワーク装置が、情報処理装置本体１０２の公開鍵情報を用いて暗号鍵情報１０４を暗号化し、情報処理装置本体１０２が、自身の秘密鍵情報で復号するようにする。

【００２５】また、例えば、磁気ディスク媒体に記録されているデジタルコンテンツ（暗号化済み）の暗号化に用いられた暗号鍵情報１０４を、情報処理装置本体１０２の製造時に、情報処理装置本体１０２の内部の不揮発性記憶装置に記録しておくという方法が挙げられる。

【００２６】同様に、図１に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、情報処理装置本体１０２および表示装置１０３は、何らかの方法によって、デジタルコンテンツ（表示データ）を暗号化／復号化するための暗号鍵情報１０５を共有する機能を有している。

【００２７】暗号鍵情報１０５を共有する方法についても、暗号鍵情報１０４を共有する方法と同様に、様々な方法が公知技術となっており、どのような方法を採用してもよい。

【００２８】例えば、情報処理装置本体１０２がデジタルコンテンツの暗号化に用いた暗号鍵情報１０５を、表示装置１０３が情報処理装置本体１０２から入手するという方法が挙げられる。このとき、情報処理装置本体１０２が、表示装置１０３の公開鍵情報を用いて暗号鍵情報で復号するようにする。

【００２９】また、例えば、暗号鍵情報１０５を、情報処理装置本体１０２および表示装置１０３の製造時に、各々の内部の不揮発性記憶装置に記録しておくという方法が挙げられる。

【００３０】また、図１に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、情報処理装置本体１０２は、（１）デジタルコンテンツ配布装置１００から配布されるデジタルコンテンツ中の暗号化部分に対して、暗号鍵情報１０４を用いて復号処理１０６を施す復号機能、（２）暗号化部分を復号後のデジタルコンテンツの展開処理１０７を行う展開機能、（３）展開したデジタルコンテンツを、表示装置１０３が要求するビットレートで出力するための表示データに変換する表示制御処理１０８を行う表示制御機能、（４）表示データの一部分に対して、暗号鍵情報１０５を用いて暗号処理１０９を施す暗号機能、を有している。

【００３１】また、図１に示すように、本実施形態に係るデジタルコンテンツ配布システムにおいては、表示装置１０３は、（１）情報処理装置本体１０２の暗号機能によって暗号化された表示データ中の暗号化部分に対して、暗号鍵情報１０５を用いて復号処理１１０を施す復号機能、（２）暗号化部分を復号後の表示データの表示処理１１１を行う表示機能、を有している。

【００３２】次に、本実施形態に係るデジタルコンテンツ配布システムの概略動作について、図２を用いて説明する。

【００３３】図２は、本実施形態に係るデジタルコンテンツ配布システムの概略動作フローチャートである。

【００３４】図２において、まず、デジタルコンテンツ配布装置１００および情報処理装置本体１０２は、何らかの方法によって、デジタルコンテンツ（配布データ）を暗号化／復号化するための暗号鍵情報１０４を共有する（ステップ２０１）。上述したように、暗号鍵情報１０４を共有する方法については、様々な方法が公知技術となっており、どのような方法を採用してもよいので、ここでは規定しない。

【００３５】続いて、デジタルコンテンツ配布装置１００は、情報処理装置本体１０２へ、暗号鍵情報１０４を用いて一部分が暗号化されたデジタルコンテンツを配布する（ステップ２０２）。上述したように、デジタルコンテンツ配布装置１００によって配布されるデジタルコンテンツは、デジタルコンテンツ配布装置１００から配布される時点で暗号化されていればよく、暗号処理を施すのがデジタルコンテンツ配布装置１００でなくてもよい。

【００３６】続いて、情報処理装置本体１０２は、デジタルコンテンツ配布装置１００から配布されたデジタルコンテンツ中の暗号化部分に対して、暗号鍵情報１０４

テップ２０３の処理によって、情報処理装置本体１０２は、その内部に、平文のデジタルコンテンツを得ることとなる。

【００３７】続いて、情報処理装置本体１０２は、ステップ２０３の処理で得られたデジタルコンテンツの展開処理１０７を行う（ステップ２０４）。例えば、ステップ２０３の処理で得られたデジタルコンテンツがＭＰＥＧ方式でフォーマッティングされているＭＰＥＧデータである場合には、ステップ２０４の処理によって、情報処理装置本体１０２は、その内部に、毎秒３０フレームからなる動画像データを得ることとなる。

【００３８】続いて、ステップ２０４の処理で得られた動画像データを含む表示データに対して、表示装置１０３が要求するビットレートで出力するための表示制御処理１０８を行う（ステップ２０５）。例えば、表示装置１０３がＴＦＴ（Thin FilmTransistor）液晶表示装置の場合は、ステップ２０５の処理では、情報処理装置本体１０２は、毎秒６０～７０フレーム程度のシーケンシャルな表示データを生成する。

【００３９】続いて、情報処理装置本体１０２および表示装置１０３は、何らかの方法によって、デジタルコンテンツ（表示データ）を暗号化／復号化するための暗号鍵情報１０５を共有する（ステップ２０６）。上述したように、暗号鍵情報１０５を共有する方法については、様々な方法が公知技術となっており、どのような方法を採用してもよいので、ここでは規定しない。

【００４０】続いて、情報処理装置本体１０２は、ステップ２０５の処理で生成した表示データ中の一部分に対して、暗号鍵情報１０５を用いて暗号処理１０９を施す（ステップ２０７）。ステップ２０７の処理によって、情報処理装置本体１０２は、その内部に、一部分が暗号化された表示データを得ることとなる。

【００４１】続いて、情報処理装置本体１０２は、表示装置１０３へ、一部分が暗号化された表示データを出力する（ステップ２０８）。

【００４２】続いて、表示装置１０３は、情報処理装置本体１０２から出力された表示データ中の暗号化部分に対して、暗号鍵情報１０５を用いて復号処理１１０を施す（ステップ２０９）。ステップ２０９の処理によって、表示装置１０３は、その内部に、平文の表示データを得ることとなる。

【００４３】続いて、表示装置１０３は、ステップ２０９の処理によって得られた表示データの表示処理１１１を行う（ステップ２１０）。ステップ２１０の処理によって、ステップ２０４の処理によって得られた動画像データを含む表示データが表示されることとなる。

【００４４】以上、ステップ２０１～ステップ２１０の処理によって、デジタルコンテンツ配布装置１００から

【００４５】なお、以下では、本実施形態に係るデジタルコンテンツ配布システムの動作のうち、ステップ２０１～ステップ２０４の処理によって実現される動作を、「配布経路暗号化」動作と称し、ステップ２０５～ステップ２１０の処理によって実現される動作を、「出力経路暗号化」動作と称する。

【００４６】また、ステップ２０６の処理は、配布経路暗号化動作に先立って行われても、並行して行われてもよい。また、ステップ２０５，ステップ２０６，ステップ２０７の処理は、情報処理装置１０１の構成によっては順番が逆転してもよい。

【００４７】次に、配布経路暗号化動作の詳細について説明する。

【００４８】まず、本実施形態に係る情報処理装置１０１の概略動作について、図３を用いて説明する。

【００４９】図３は、本実施形態に係る情報処理装置１０１の概略構成図である。

【００５０】図３では、パーソナルコンピュータ（ＰＣ）などの情報処理装置１０１のうち、表示に関する部分であって、かつ、配布経路暗号化動作に関する部分のみを示している。

【００５１】図中、１０２は情報処理装置本体、１０３は表示装置、１０４は暗号鍵情報、３０１は中央演算装置（ＣＰＵ：Central Processing Unit）、３０２はシステムメモリ、３０３は表示制御装置、３０４は表示メモリ、３０５は入力制御装置、３０６は通信制御装置、３０７はバス、３０８は復号処理部、３０９はコンテンツ展開処理部である。

【００５２】図３において、デジタルコンテンツ配布装置１００がネットワーク装置である場合には、通信制御装置３０６が、ＣＰＵ３０１の指示に従って、デジタルコンテンツを入力する。また、デジタルコンテンツ配布装置１００が記録媒体である場合には、入力制御装置３０５が、ＣＰＵ３０１の指示に従って、デジタルコンテンツを入力する。通信制御装置３０６または入力制御装置３０５が入力したデジタルコンテンツは、ＣＰＵ３０１の指示に従って、バス３０７を介して表示制御装置３０３に入力される。

【００５３】表示制御装置３０３においては、復号処理部３０８が、入力したデジタルコンテンツ中の暗号化部分に対して、表示制御装置３０３の内部に保持されている暗号鍵情報１０４を用いて復号処理１０６を施し、表示制御装置３０３の内部に、平文のデジタルコンテンツを得る。続いて、コンテンツ展開処理部３０９が、復号処理部３０８が復号したデジタルコンテンツの展開処理１０７を行い、表示制御装置３０３の内部に、展開されたデジタルコンテンツを得る。

【００５４】ここまでの動作が配布経路暗号化動作に相

【0055】なお、復号処理部308およびコンテンツ展開処理部309は、表示制御装置303内にハードウェアとして実装されるようにしてもよいし、また、表示制御装置303内に独自のCPUおよびメモリを設け、ソフトウェアとして実装されるようにしてもよい。

【0056】次に、配布経路暗号化動作で、デジタルコンテンツ配布装置100から配布されるデジタルコンテンツの暗号化方法の一例について、図5および図6を用いて説明する。

【0057】図5は、デジタルコンテンツ配布装置100から配布されるデジタルコンテンツの暗号化方法の一例を示す説明図であり、図6は、図5に示す暗号化方法で暗号化されたデジタルコンテンツを表示装置103で表示した場合の表示イメージを示す説明図である。

【0058】図5および図6では、デジタルコンテンツがMPEGデータである場合を例にしている。

【0059】MPEG方式による圧縮では、例えば、1フレームm×n画素，毎秒kフレームから構成される動画像データは、Iピクチャ形式，Pピクチャ形式，Bピクチャ形式の3つの形式に分類される。

【0060】（1）Iピクチャ形式

Iピクチャ形式では、1フレームm×n画素の画像データは、8×8画素の複数のブロックに分割され、各ブロックごとに直交変換処理が施されて周波数領域データに変換された後、量子化されてデータ圧縮が行われる。Iピクチャデータでは、元フレーム内のデータのみを対象にした符号化がなされており、Iピクチャデータからは、展開処理によって1枚のフレームデータが得られる。

【0061】（2）Pピクチャ形式

Pピクチャ形式では、順方向のフレーム間予測を行ったデータ圧縮が行われる。Pピクチャデータでは、Iピクチャとの差分情報を用いた符号化がなされており、元フレームの復元には、Pピクチャデータ，元画となるIピクチャデータが必要となる。すなわち、Pピクチャデータのみでは画像データは得られない。

【0062】（3）Bピクチャ形式

Bピクチャ形式では、双方向のフレーム間予測を行ったデータ圧縮が行われる。Bピクチャデータでは、IピクチャとPピクチャとの間の差分情報を用いた符号化がなされており、元フレームの復元には、Pピクチャデータ、元画となるIピクチャデータ，Bピクチャデータが必要となる。すなわち、Bピクチャデータのみでは画像データは得られない。

【0063】また、1ピクチャデータの符号割り当て量は、図5に示すように、Iピクチャ，Pピクチャ，Bピクチャの順に小さくなる。動画像データは、フレームごとに、例えば、IBB，PBB，PBB，IBB，PBB，PBBなどの順番に符号化される。

暗号化方法としては、以下の3つの方法が考えられる。

【0065】（1）第1の暗号化方法

第1の暗号化方法としては、Iピクチャデータのみを暗号化するという方法がある。第1の暗号化方法は、さらに、圧縮単位となるブロックごとに暗号化を施す／施さないという方法、および、圧縮単位となるブロック内の周波数成分に着目し、高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法に分けられる。

【0066】まず、前者の方法（圧縮単位となるブロックごとに暗号化を施す／施さないという方法）について説明すると、例えば、図6（a）に示す元画像に対して、本方法による暗号化を行う際には、ブロックを暗号処理の処理対象とし、あるブロックには暗号処理を施し、あるブロックには暗号処理を施さないようにする。

【0067】本方法により暗号化されたMPEGデータは、暗号鍵情報104を用いた復号処理を施さなければ、表示装置103に表示される際のイメージは、図6（b）に示すようになる。本方法では、暗号化を施すブロック数を増減させることで、元画像の汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。

【0068】次に、後者の方法（高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法）について説明すると、例えば、図6（a）に示す元画像に対して、本方法による暗号化を行う際には、ブロック内の低周波領域データを暗号処理の処理対象とし、各ブロック中の低周波領域データには暗号処理を施し、高周波領域データには暗号処理を施さないようにする。本方法により暗号化されたMPEGデータは、暗号鍵情報104を用いた復号処理を施さなければ、表示装置103に表示される際のイメージは、図6（c）に示すようになる。

【0069】低周波数領域データを暗号化すると、図6（c）に示すように、元画像は大きく汚染され、元画像を観測するのは困難となるが、高周波数領域データを暗号化すると、図示していないが、元画像にノイズが重畳されたイメージとなる。

【0070】本方法では、暗号化を施す周波数領域を選択することで、元画像の汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。また、全てのブロックを暗号処理の処理対象としなくても、一部のブロックを暗号処理の処理対象としてもよい。

【0071】第1の暗号化方法によってIピクチャデータのみを暗号化した場合、暗号鍵情報104がないとIピクチャデータを復元することができず、従って、図5に示すように、Iピクチャデータの差分情報であるPピクチャデータおよびBピクチャデータも、暗号化されて

えば、ＩＢＢ，ＰＢＢ，ＰＢＢ，ＩＢＢ，ＰＢＢ，ＰＢＢの順番に符号化された動画像データは、暗号鍵情報１０４がない場合には、×××，×××，×××，×××，×××，×××（×は正常な復号・展開の失敗を意味する。）となって、全てのフレーム共に正常な元画像が得られない。

【００７２】（２）第２の暗号化方法

第２の暗号化方法としては、Ｐピクチャデータのみを暗号化するという方法がある。第２の暗号化方法も、第１の暗号化方法と同様に、さらに、圧縮単位となるブロックごとに暗号化を施す／施さないという方法、および、圧縮単位となるブロック内の周波数成分に着目し、高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法に分けられる。

【００７３】第２の暗号化方法によってＰピクチャデータのみを暗号化した場合、暗号鍵情報１０４がないとＰピクチャデータを復元することができず、従って、図５に示すように、Ｉピクチャデータ，Ｐピクチャデータの差分情報であるＢピクチャデータも、暗号化されてはいないが、これを展開することも不可能となる。例えば、ＩＢＢ，ＰＢＢ，ＰＢＢ，ＩＢＢ，ＰＢＢ，ＰＢＢの順番に符号化された動画像データは、暗号鍵情報１０４がない場合には、Ｉ××，×××，×××，Ｉ××，×××，×××（×は正常な復号・展開の失敗を意味する。）となって、得られる正常な画像フレームはＩピクチャデータのみとなる。

【００７４】（３）第３の暗号化方法

第３の暗号化方法としては、Ｂピクチャデータのみを暗号化するという方法がある。第３の暗号化方法も、第１の暗号化方法と同様に、さらに、圧縮単位となるブロックごとに暗号化を施す／施さないという方法、および、圧縮単位となるブロック内の周波数成分に着目し、高周波領域データ／低周波領域データごとに暗号化を施す／施さないという方法に分けられる。

【００７５】第３の暗号化方法によってＢピクチャデータのみを暗号化した場合、図５に示すように、暗号鍵情報１０４がないとＢピクチャデータを復元することができない。例えば、ＩＢＢ，ＰＢＢ，ＰＢＢ，ＩＢＢ，ＰＢＢ，ＰＢＢの順番に符号化された動画像データは、暗号鍵情報１０４がない場合には、Ｉ××，Ｐ××，Ｐ××，Ｉ××，Ｐ××，Ｐ××（Ｘは正常な復号・展開の失敗を意味する。）となって、得られる正常な画像フレームはＩピクチャデータおよびＰピクチャのみとなる。

【００７６】以上、ＭＰＥＧデータの暗号化方法として３つの方法を説明したが、これらの方法を任意に組み合わせるようにしてもよい。

【００７７】本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作において、デジタルコンテンツデータを暗号化するようにしているので、正当な暗号鍵情報１０４を有していない場合には、元画像の一部分が汚損した状態となる。一部分が汚損されたデジタルコンテンツは、その価値が損なわれるので、デジタルコンテンツの不正コピーを防止することが可能となり、また、デジタルコンテンツの一部分が開示されるので、ユーザの視聴要求を刺激し、デジタルコンテンツの完全な視聴を促すことが可能となる。

【００７８】特に、本実施形態に係るデジタルコンテンツ配布システムにおいては、暗号処理の処理対象とするデータを選択する際に、そのフォーマットに着目するようにしている。すなわち、デジタルコンテンツを単なるビット列として暗号処理の処理対象とした場合、ヘッダ，ペイロード，フッタと言ったデータ構造が全て失われてしまい、デジタルコンテンツとして利用することがまったく不可能となってしまうが、本実施形態に係るデジタルコンテンツ配布システムにおいては、デジタルコンテンツを単なるビット列として扱うのではなく、暗号処理の処理対象とするデータを、フォーマットの有意味部分に合わせて選択するようにしているので、データ全体ではなく、一部分だけの汚損が可能となっている。

【００７９】また、本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作において、データ汚損に、暗号鍵情報１０４を用いた暗号処理を利用していることから、ユーザの視聴欲求を刺激するために、完全なデジタルコンテンツとは別に汚損デジタルコンテンツを用意する必要がなく、デジタルコンテンツの配布・蓄積に掛かるコストを低減することが可能となる。

【００８０】さらに、本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作において、デジタルコンテンツの一部分だけを暗号処理の処理対象とし、デジタルコンテンツ全体に対する暗号処理を避けることによって、暗号処理／復号処理の処理量の軽減も可能となっている。なお、汚損度と処理量とはトレードオフの関係にあり、要求に応じて優先度の変更が容易に可能である。

【００８１】以上説明したように、本実施形態に係るデジタルコンテンツ配布システムによれば、配布経路暗号化動作によって、デジタルコンテンツの配布経路上で著作権を保護しつつ、ユーザの視聴欲求を刺激することが可能となる。

【００８２】なお、本実施形態に係る情報処理装置１０１は、図３に示す構成ではなく、図７に示す構成にし、図３に示した復号処理部３０８およびコンテンツ展開処理部３０９を、ソフトウェアで実現するようにしてもよい。

【００８３】図７は、本実施形態に係る情報処理装置１

処理装置１０１のうち、表示に関する部分であって、かつ、配布経路暗号化動作に関する部分のみを示している。

【００８５】図中、図３と同じ構成要素には同じ符号を付与してある。７０１は不揮発性記憶装置である。

【００８６】図７に示す構成の情報処理装置１０１においては、図３に示した復号処理部３０８およびコンテンツ展開処理部３０９の動作を、ＣＰＵ３０１がシステムメモリ３０２上にプログラムをロードして実行することで実現するものである。

【００８７】図７において、デジタルコンテンツ配布装置１００がネットワーク装置である場合には、通信制御装置３０６が、ＣＰＵ３０１の指示に従って、デジタルコンテンツを入力する。また、デジタルコンテンツ配布装置１００が記録媒体である場合には、入力制御装置３０５が、ＣＰＵ３０１の指示に従って、デジタルコンテンツを入力する。通信制御装置３０６または入力制御装置３０５が入力したデジタルコンテンツは、ＣＰＵ３０１の指示に従って、バス３０７を介してシステムメモリ３０２に入力される。

【００８８】ＣＰＵ３０１は、入力したデジタルコンテンツ中の暗号化部分に対して、暗号鍵情報１０４を用いて復号処理１０６を施し、システムメモリ３０２上に、平文のデジタルコンテンツを得る。続いて、ＣＰＵ３０１は、復号したデジタルコンテンツの展開処理１０７を行い、展開されたデジタルコンテンツを得る。得られたデジタルコンテンツは表示制御装置３０３に入力される。

【００８９】ここで、暗号鍵情報１０４は、図３を用いた説明では、表示制御装置３０３の内部に保持されているものとしたが、図７に示す構成の情報処理装置１０１においては、暗号鍵情報１０４の共有も、ＣＰＵ３０１がシステムメモリ３０２上にプログラムをロードして実行することで実現するものとする。

【００９０】また、本実施形態に係る情報処理装置１０１は、図３および図７のいずれにおいても、情報処理装置１０２本体と表示装置１０３とを備えた構成としているが、情報処理装置本体１０２と表示装置１０３が一体化した構成であってもよい。すなわち、本実施形態に係る情報処理装置１０１を、いわゆるＰＤＡ（PersonalDigital Assistant）などと呼ばれる携帯情報端末としてもよい。

【００９１】一般に、携帯情報端末は、比較的性能の低いＣＰＵや小容量のメモリなどを用いて構成されることが多いので、比較的重い処理である暗号処理は携帯情報端末にとって大きな負担になるという問題がある。

【００９２】そこで、このような問題がある携帯情報端末を、本実施形態に係るデジタルコンテンツ配布システムで用いるようにすれば、全体ではなく一部分が暗号化目的とする、著作権保護とユーザの視聴覚欲求刺激の両立を実現することができる上、暗号処理量の低減による負荷低下効果を得ることができる。特に、携帯情報端末が暗号処理をソフトウェアで実現する場合には、暗号処理用に高性能なＣＰＵや大容量メモリを搭載する必要がなくなり、低コスト化，低消費電力化といった効果が得られる。また、携帯情報端末が暗号処理専用のハードウェアを備えるようにする場合には、暗号処理専用のハードウェアに必要な処理速度が低下することから、低動作速度による低消費電力化，ハードウェア論理の小規模化による低コスト化といった効果が得られる。

【００９３】ところで、上述の説明では、ＭＰＥＧデータ（動画像データ）を例にしたが、必ずしも動画像データのみを対象としている訳ではない。

【００９４】例えば、デジタルコンテンツがＪＰＥＧデータ（静止画像データ）である場合には、上述したＩピクチャデータの暗号化方法と同様の暗号化方法を用いることが可能である。

【００９５】また、例えば、デジタルコンテンツがＭＰＥＧデータ（音声データ）である場合には、音声情報に対して帯域分割を施し、分割された周波数成分ごとに独立した符号化を行っていることから、低周波成分のみに対する暗号化／高周波成分のみに対する暗号化を行うようにしたり、数サンプルおきに暗号化を行うようしたりすればよい。このようにしてデータ汚損度を制御すれば、適度に耳障りな再生音を生成することが可能となる。

【００９６】さて、次に、出力経路暗号化動作の詳細について説明する。

【００９７】まず、本実施形態に係る情報処理装置１０１の概略動作について、図４を用いて説明する。

【００９８】図４は、本実施形態に係る情報処理装置１０１の概略構成図である。

【００９９】図４では、ＰＣなどの情報処理装置１０１のうち、表示に関する部分であって、かつ、出力経路暗号化動作に関する部分のみを示している。

【０１００】図中、図３と同じ構成要素には同じ符号を付与してある。４０１は暗号処理部、４０２は復号処理部、４０３はデータドライバである。

【０１０１】ここでは、表示装置１０３は、例えば、液晶表示（ＬＣＤ：Liquid Crystal Display）装置や、デジタル／アナログ変換機能を具備したＣＲＴ（Cathode-RayTube）装置のような、デジタル入力の表示装置とする。

【０１０２】図４において、上述した配布経路暗号化動作によって表示制御装置３０３の内部に展開されたデジタルコンテンツを含む表示データ（平文表示データ）は、ＣＰＵ３０１の指示に従って、表示メモリ３０４に蓄積される。

部４０１が、表示メモリ３０４に蓄積された平文表示データを入力し、入力した平文表示データの一部分に対して、表示制御装置３０３の内部に保持されている暗号鍵情報１０５を用いて暗号処理１０９を施し、表示制御装置３０３の内部に、暗号化された表示データを得る。得られた暗号化表示データは、表示制御装置３０３から表示装置１０３へ入力される。

【０１０４】続いて、表示装置１０３においては、復号処理部４０２が、入力した暗号化表示データ中の暗号化部分に対して、表示装置１０３の内部に保持されている暗号鍵情報１０５を用いて復号処理１１０を施し、表示装置１０３の内部に、平文表示データを得る。続いて、データドライバ４０３が、復号処理部４０２が復号した平文表示データを、表示画面上の各々の表示画素に供給することで、平文表示データの表示処理１１１を行う。

【０１０５】以上の動作が出力経路暗号化動作に相当している。

【０１０６】なお、暗号処理部４０２は、表示制御装置３０３内にハードウェアとして実装されるようにしてもよいし、また、表示制御装置３０３内に独自のＣＰＵおよびメモリを設け、ソフトウェアとして実装されるようにしてもよい。

【０１０７】次に、本実施形態に係る表示制御装置３０３の概略動作について、図８を用いて説明する。

【０１０８】図８は、本実施形態に係る表示制御装置３０３の概略構成図である。

【０１０９】図８では、表示制御装置３０３のうち、出力経路暗号化動作に関する部分のみを示している。

【０１１０】図中、８０１はメモリ制御部、８０２はタイミング生成部、８０３はタイミング信号、８０４はメモリ制御信号、８０５はメモリアドレス信号、３０４は表示メモリ、８０６はＬＣＤ制御部、８０７はＬＣＤ制御信号、８０８は平文表示データ、８０９はタイミング制御部、８１０はＬＣＤ表示データ、８１１はシリアル／パラレル変換回路（Ｓ／Ｐ回路）、８１２はＳ／Ｐ済ＬＣＤ表示データ、８１３は暗号化Ｓ／Ｐ済ＬＣＤ表示データ、８１４はパラレル／シリアル変換回路（Ｐ／Ｓ回路）、８１５は暗号化ＬＣＤ表示データ、８１６は遅延回路、８１７は遅延済ＬＣＤ制御信号である。

【０１１１】図８において、メモリ制御部８０１は、タイミング生成部８０２から送られてくるタイミング信号８０３を用いて、メモリ制御信号８０４およびメモリアドレス信号８０５を生成し、表示メモリ３０４から平文表示データ８０８を順次読み出す。

【０１１２】一方、ＬＣＤ制御部８０６は、タイミング生成部８０２から送られてくるタイミング信号８０３を用いて、ＬＣＤの表示タイミングを制御するＬＣＤ制御信号８０７を生成する。

制御信号８０７による表示タイミングに合わせて、ＬＣＤ表示データ８１０として送り出す。

【０１１４】すなわち、表示メモリ３０４から読み出された平文表示データ８０８は、タイミング制御部８０９によって、ＬＣＤ制御信号８０７に同期したＬＣＤ表示データ８１０となる。

【０１１５】例えば、ＬＣＤ制御信号８０７が、１データ転送クロック同期で１画素分の表示データを転送し、かつ、１画素が１６ビットのデータから構成されているとすると、ＬＣＤ表示データ８１０は、１６ビットデータバスとなる。ここで、暗号処理に、例えば、ＤＥＳのようなブロック暗号を用いた場合、暗号処理部４０１は、暗号鍵情報１０５を用いて、６４ビット単位のブロック暗号処理を施すこととなる。

【０１１６】両者の処理単位の違いを吸収するために、本実施形態に係る表示制御装置３０３においては、Ｓ／Ｐ回路８１２およびＰ／Ｓ回路８１４を用いている。Ｓ／Ｐ回路８１１は、ＬＣＤ表示データ８１０のデータ幅（ここでは、１６ビット単位）を、暗号処理単位（ここでは、６４ビット単位）幅に変換し、Ｓ／Ｐ済ＬＣＤ表示データ８１２として暗号処理部４０１に供給するものであり、また、Ｐ／Ｓ回路８１４は、暗号処理部４０１によって暗号処理が施された後の暗号化Ｓ／Ｐ済ＬＣＤ表示データ８１３のデータ幅を、ＬＣＤ表示データ８１０のデータ幅に変換し、暗号化ＬＣＤ表示データ８１５としてデータドライバ４０３に供給するものである。

【０１１７】ＬＣＤ表示データ８１０のデータ幅と暗号処理部４０１の暗号処理単位幅とに応じて、Ｓ／Ｐ回路８１１およびＰ／Ｓ回路８１４の構成は異なる。

【０１１８】図８に示すように、本実施形態に係る表示制御装置３０３においては、Ｓ／Ｐ回路８１１，暗号処理部４０１，Ｐ／Ｓ回路８１４による処理が設けられているので、これらの処理による遅延と同等の遅延を、遅延回路８１６によって、ＬＣＤ制御部８０６が生成したＬＣＤ制御信号８０７に加え、遅延済ＬＣＤ制御信号８１７として出力するようにすることで、Ｐ／Ｓ回路８１４から出力される暗号化ＬＣＤ表示データ８１６が、遅延済ＬＣＤ制御信号８１７に同期してデータドライバ４０３に供給されるようにしている。

【０１１９】これにより、表示制御装置３０３による表示タイミング制御の処理途上で、表示データの一部分に対して暗号処理を施すこと、すなわち、ＬＣＤ表示データ８１０のリアルタイム暗号処理による暗号化ＬＣＤ表示データ８１５の作成が可能となる。

【０１２０】次に、本実施形態に係る表示装置１０３の概略動作について、図９を用いて説明する。

【０１２１】図９は、本実施形態に係る表示装置１０３の概略構成図である。

力経路暗号化動作に関する部分（すなわち、データドライバ４０３に相当する液晶駆動ドレイン側ドライバ）のみを示している。

【０１２３】図中、９０１は暗号化表示データの取り込み信号（ＣＬ２信号）、９０２は暗号化表示データ、９０３はＬＣＤ駆動電圧を出力するタイミング信号（ＣＬ１信号）、９０４はＬＣＤ駆動用電源、９０５は液晶駆動出力信号、９０６はラッチアドレスセレクタ、９０７はラッチ回路－１、９０８はラッチ回路－２、９０９は回路駆動電圧から液晶駆動電圧へ昇圧するレベルシフタ、９１０は液晶駆動用の電圧レベルを発生する液晶駆動回路、９１１はラッチ回路－３、９１２は平文表示データである。

【０１２４】図９において、ラッチアドレスセレクタ９０６は、暗号化表示データ９０２の入力と同期して表示制御装置３０３から入力したＣＬ２信号９０１（図８に示した遅延済ＬＣＤ制御信号８１７に相当している。）の立下りをカウントすることで、ラッチ回路－１（９０７）に対するラッチ信号を生成する。

【０１２５】表示制御装置３０３から入力した暗号化表示データ９０２は、ラッチアドレスセレクタ９０６が生成するラッチ信号によって、ラッチ回路－１（９０７）上に入力順に保持されていく。

【０１２６】ＣＬ１信号９０３は、表示１ラインごとに入力する水平同期信号であり、ＣＬ１信号９０３の入力によって、ラッチ回路－１（９０７）上にラッチされた１表示ライン分の暗号化表示データ９０２は、１ライン表示期間ごとに、１ライン分ずつ、ラッチ回路－２（９０８）上にラッチされる。

【０１２７】ラッチ回路－２（９０８）上にラッチされた１ライン分の暗号化表示データ９０２は、復号処理部４０２によって、暗号鍵情報１０５を用いた復号処理１００が施されて平文表示データ９１２となり、ＣＬ１信号９０３によって、１ライン表示期間ごとに、１ライン分ずつ、ラッチ回路－３（９１１）上にラッチされる。

【０１２８】ラッチ回路－３（９１１）上にラッチされた１ライン分の平文表示データ９１２は、レベルシフタ９０９および液晶駆動回路９１０を介して液晶駆動電圧に変換され、１ライン表示期間、液晶に印加される。

【０１２９】以上の処理により、１ラインごとに液晶への表示動作が実行される。

【０１３０】ここで、復号処理に、例えば、ＤＥＳのようなブロック暗号を用いた場合、復号処理部４０２は、ラッチ回路－２（９０８）から出力されるビット数を、同時に並列処理可能な分だけ、ブロック単位に並列させる。例えば、液晶駆動ドレイン側ドライバが、１ライン当たり１０２４画素構成で１画素当たり１８ビット出力であるとすると、１ライン当たり１８４３２ビットとなるので、６４ビット単位（ＤＥＳによる処理単位）のブ２は、暗号鍵情報１０５を用いて、６４ビット単位のブロック復号処理を施すこととなる。

【０１３１】これにより、表示装置１０３の液晶駆動ドレイン側ドライバによる表示制御の処理途上で、表示データの一部分に対して復号処理を施すこと、すなわち、暗号化表示データ９１２のリアルタイム復号処理による平文表示データ９１２の作成・表示が可能となる。

【０１３２】なお、本実施形態に係る表示装置１０３は、図９に示す構成ではなく、図１０に示す構成にしてもよい。

【０１３３】図１０は、本実施形態に係る表示装置１０３の他の概略構成図である。

【０１３４】図１０でも、図９と同様に、表示装置１０３が液晶表示装置である場合を例にしており、表示装置１０３のうち、出力経路暗号化動作に関する部分（すなわち、データドライバ４０３に相当する液晶駆動ドレイン側ドライバ）のみを示している。

【０１３５】図中、図９と同じ構成要素には同じ符号を付与してある。１００１はＳ／Ｐ回路、１００２はＰ／Ｓ回路、１００３はＳ／Ｐ済表示データ、１００４は平文表示データである。

【０１３６】図１０に示す表示装置１０３は、暗号化表示データ９０２のデータ幅が、１画素当たりのデータビット数とデータ転送クロック（ＣＬ２信号９０１）とに依存し、復号処理部４０２の復号処理単位のデータ幅と異なっている場合に、Ｓ／Ｐ回路１００１によって、暗号化表示データ９０２のデータ幅を適切な復号処理単位のデータ幅に変換し、Ｓ／Ｐ済表示データ１００３としてから、復号処理部４０２によって、暗号鍵情報１０５を用いて復号処理を行い、復号処理によって得られた平文表示データ１００４を、Ｐ／Ｓ回路１００２によって、平文表示データ９１２のデータ幅に変換するようにしたものである。

【０１３７】復号処理部４０２は、最低１ブロックを処理できればよく、１画素当たりの暗号化表示データ９０２のビット数とＣＬ２信号９０１とに応じて、処理ブロックを並列させるようにしてもよい。

【０１３８】以上、表示装置１０３が液晶表示装置である場合を例にとって、出力経路暗号化動作について説明したが、表示装置１０３が、例えば、デジタル入力でデジタル／アナログ変換部を具備するＣＲＴ装置である場合でも、デジタル処理を行う途上で、同様の復号処理を行うようにすれば、平文表示データの作成・表示が可能となる。

【０１３９】次に、出力経路暗号化動作で、表示制御装置３０３から出力される表示データの暗号化方法の一例について、図１１および図１２を用いて説明する。

【０１４０】図１１は、表示制御装置３０３から出力される表示データの暗号化方法の一例を示す説明図であ

た場合の表示イメージを示す説明図である。

【０１４１】図１１では、元画像（本来の平文表示データ）の暗号化方法として、ライン方向に暗号処理を施す暗号化方法と、カラム方向に暗号処理を施す暗号化方法とを示している。

【０１４２】（１）ライン方向に暗号処理を施す暗号化方法

例えば、図１１（ａ）に示す元画像（本来の平文表示データ）に対して、本方法による暗号化を行う際には、ライン方向に、複数ライン分（例えば、数ライン程度）の表示データを１単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すようにする。具体的には、数ライン分の表示データごとに、交互に、暗号処理を施す場合と暗号処理を施さない場合とを繰り返すようにする。

【０１４３】本方法により暗号化された表示データは、暗号鍵情報１０５を用いた復号処理を施せば、表示装置１０３に表示される際のイメージは、図１１（ａ）に示す元画像と同じイメージになるが、暗号鍵情報１０５を用いた復号処理を施さなければ、表示装置１０３に表示される際のイメージは、図１１（ｂ）に示すように、数ラインおきに数ライン分が汚損された表示データとなる。

【０１４４】本方法では、１単位とするライン数を予め決定しておき、決定したライン数ごとに、表示制御装置３０３の暗号処理部４０１が選択的に暗号化すると共に、表示装置１０３の復号処理部４０２が選択的に復号するようにする。これにより、表示データの一部に対する汚損が可能となり、また、表示制御装置３０３の暗号処理部４０１および表示装置１０３の復号処理部４０２における暗号／復号処理量の削減が可能となる。

【０１４５】また、１単位とするライン数を増減させることで、表示データの汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。

【０１４６】（２）カラム方向に暗号処理を施す暗号化方法

例えば、図１１（ａ）に示す元画像（本来の平文表示データ）に対して、本方法による暗号化を行う際には、カラム方向に、複数カラム分（例えば、数カラム程度）の表示データを１単位とし、これらの単位の一部の単位を暗号処理の処理対象として、暗号処理を施すようにする。具体的には、数カラム分の表示データごとに、交互に、暗号処理を施す場合と暗号処理を施さない場合とを繰り返すようにする。

【０１４７】本方法により暗号化された表示データは、暗号鍵情報１０５を用いた復号処理を施せば、表示装置１０３に表示される際のイメージは、図１１（ａ）に示す元画像と同じイメージになるが、暗号鍵情報１０５を用いた復号処理を施さなければ、表示装置１０３に表示される際のイメージは、図１１（ｂ）に示すように、数カラムおきに数カラム分が汚損された表示データとなる。

【０１４８】本方法では、１単位とするカラム数を予め決定しておき、決定したカラム数ごとに、表示制御装置３０３の暗号処理部４０１が選択的に暗号化すると共に、表示装置１０３の復号処理部４０２が選択的に復号するようにする。これにより、表示データの一部に対する汚損が可能となり、また、表示制御装置３０３の暗号処理部４０１および表示装置１０３の復号処理部４０２における暗号／復号処理量の削減が可能となる。

【０１４９】また、１単位とするカラム数を増減させることで、表示データの汚損度合を制御可能であり、どの程度の開示を行うかを自由に変更することができる。

【０１５０】図１２は、表示制御装置３０３から出力される表示データの暗号化方法の一例を示す説明図であり、図１２では、元画像（本来の平文表示データ）中の１画素分の表示データについて、その一部分に対して暗号処理を施す暗号化方法を示している。

【０１５１】本方法では、１画素内の表示データ中の上位ビットのみに暗号処理を施すようにするか、または、１画素内の表示データ中の下位ビットのみに暗号処理を施すようにする。

【０１５２】上位ビットのみを暗号化し、下位ビットは平文のままとした場合は、表示データの変化量が大きくなる。そこで、暗号化表示データを復号せずに表示装置１０３上で表示すると、データの汚損度が大きく、表示データの観察は困難となる。

【０１５３】また、下位ビットのみを暗号化し、上位ビットは平文のままとした場合は、表示データの変化量は少ない。そこで、暗号化表示データを復号せずに表示装置１０３上で表示すると、データの汚損度が小さく、画面上のちらつきとして観察されるが、表示データのおおまかな観察は可能である。

【０１５４】図１２では、１画素分の表示データが８ビットで構成され、ある平文表示データが「５５ｈ」であるとしたときに、上位ビットのみを暗号化して「５５ｈ」が「ｅ５ｈ」になり、下位ビットのみを暗号化して「５５ｈ」が「５２ｈ」になった例を示した。このように、上位ビットのみを暗号化する方が、平文表示データからの変化量が大きくなるので、より異なった表示として観測されることとなる。

【０１５５】本方法では、上位ビットのみを暗号化するか、または、下位ビットのみを暗号化するかを選択することで、表示データの汚損度合を選択することが可能であり、また、表示制御装置３０３の暗号処理部４０１および表示装置１０３の復号処理部４０２における暗号／復号処理量の削減が可能となる。

【０１５６】以上、ライン方向／カラム方向に暗号処理

法について説明したが、これらの方法を任意に組み合わせるようにしてもよい。

【０１５７】本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作によって、従来は行われていなかった、最終出力装置である表示装置１０３への出力経路でのデジタルコンテンツの著作権保護が可能となる。

【０１５８】そして、本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作において、デジタルコンテンツ（表示データ）を単純に暗号化するのではなく、暗号処理の処理対象とするデータを選択し、一部分のみを暗号化するようにしているので、正当な暗号鍵情報１０５を有していない場合には、元画像の一部分が汚損した状態となる。一部分が汚損されたデジタルコンテンツは、その価値が損なわれるので、デジタルコンテンツの不正コピーを防止することが可能となり、また、デジタルコンテンツの一部分が開示されるので、ユーザの視聴要求を刺激し、デジタルコンテンツの完全な視聴を促すことが可能となる。

【０１５９】さらに、本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作において、デジタルコンテンツの一部分だけを暗号処理の処理対象とし、デジタルコンテンツ全体に対する暗号処理を避けることによって、暗号処理／復号処理の処理量の軽減も可能となっている。なお、汚損度と処理量とはトレードオフの関係にあり、要求に応じて優先度の変更が容易に可能である。

【０１６０】以上説明したように、本実施形態に係るデジタルコンテンツ配布システムによれば、出力経路暗号化動作によって、デジタルコンテンツの出力経路上で著作権を保護しつつ、ユーザの視聴欲求を刺激することが可能となる。

【０１６１】なお、本実施形態に係る情報処理装置１０１は、図４に示す構成ではなく、図１３に示す構成にし、図４に示した暗号処理部４０１を、ソフトウェアで実現するようにしてもよい。

【０１６２】図１３は、本実施形態に係る情報処理装置１０１の他の概略構成図である。

【０１６３】図１３でも、図４と同様に、ＰＣなどの情報処理装置１０１のうち、表示に関する部分であって、かつ、出力経路暗号化動作に関する部分のみを示している。

【０１６４】図中、図４と同じ構成要素には同じ符号を付与してある。７０１は不揮発性記憶装置である。

【０１６５】図１３に示す構成の情報処理装置１０１においては、図４に示した暗号処理部４０１の動作を、ＣＰＵ３０１がシステムメモリ３０２上にプログラムをロードして実行することで実現するものである。すなわち、図１３に示す構成の情報処理装置１０１は、表示制御装置３０３が暗号化表示データを暗号化するようにしている。

【０１６６】図１４は、図１３に示す構成の情報処理装置１０１の概略動作を示す説明図である。

【０１６７】図１４に示すように、表示メモリ３０４に蓄積された平文表示データ８０８は、ＣＰＵ３０１の指示に従って、表示制御装置３０３およびバス３０７を介してシステムメモリ３０２に入力される。

【０１６８】ＣＰＵ３０１は、入力した平文表示データ８０８に対して、暗号鍵情報１０５を用いて暗号処理１０９を施す。ＣＰＵ３０１によって暗号化された暗号化表示データ９０２は、バス３０７および表示制御装置３０３を介して表示メモリ３０４にに入力される。表示メモリ３０４に蓄積された暗号化表示データ９０２は、表示制御装置３０３によって読み出され、表示装置１０３に出力される。

【０１６９】すなわち、図１３に示す構成の情報処理装置１０１においては、ＣＰＵ３０１が、表示メモリ３０４上に平文表示データ８０８を生成し、さらに、平文表示データ８０８から表示メモリ３０４上に暗号化表示データ９０２を生成する。表示制御装置３０３は、暗号化表示データ９０２の読み出し動作を行い、表示動作を行う。

【０１７０】ここで、暗号鍵情報１０５は、図４を用いた説明では、表示制御装置３０３の内部に保持されているものとしたが、図１３に示す構成の情報処理装置１０１においては、暗号鍵情報１０５は、不揮発性記憶装置７０１に保持されているものとする。

【０１７１】また、本実施形態に係る情報処理装置１０１は、図４および図１３のいずれにおいても、情報処理装置１０２本体と表示装置１０３とを備えた構成としているが、配布経路暗号化動作で説明したのと同様に、情報処理装置本体１０２と表示装置１０３が一体化した構成であってもよい。すなわち、本実施形態に係る情報処理装置１０１を、いわゆるＰＤＡなどと呼ばれる携帯情報端末としてもよい。

【０１７２】上述したように、一般に、携帯情報端末は、比較的性能の低いＣＰＵや小容量のメモリなどを用いて構成されることが多いので、比較的重い処理である暗号処理は携帯情報端末にとって大きな負担になるという問題がある。

【０１７３】そこで、このような問題がある携帯情報端末を、本実施形態に係るデジタルコンテンツ配布システムで用いるようにすれば、全体ではなく一部分が暗号化されたデジタルコンテンツを扱うことにより、本発明が目的とする、著作権保護とユーザの視聴覚欲求刺激の両立を実現することができる上、暗号処理量の低減による負荷低下効果を得ることができる。特に、携帯情報端末が暗号処理をソフトウェアで実現する場合には、暗号処理用に高性能なＣＰＵや大容量メモリを搭載する必要がなくなり、低コスト化、低消費電力化といった効果が得

られる。また、携帯情報端末が暗号処理専用のハードウェアを備えるようにする場合には、暗号処理専用のハードウェアに必要な処理速度が低下することから、低動作速度による低消費電力化，ハードウェア論理の小規模化による低コスト化といった効果が得られる。

【０１７４】ところで、上述の説明では、デジタル表示装置への出力を例にしたが、必ずしも表示のみを対象としている訳ではない。

【０１７５】例えば、デジタル入力を持った音声出力装置においても、ＰＣＭ（Pulse CodeModulation）符号化された音声データに対して、同様に、数サンプルおきに暗号化を施すことで、出力装置経路暗号化動作を実現することが可能である。

【０１７６】以上説明したように、本実施形態に係るデジタルコンテンツ配布システムは、デジタルコンテンツのフォーマットに依存する形で、デジタルコンテンツの一部分に対して暗号処理を施すようにすることで、正当な暗号鍵情報を有さない場合に、一部が汚損されたデジタルコンテンツとなるようにしている。そこで、デジタルコンテンツの著作権を保護しつつ、ユーザの視聴覚欲求を刺激することが可能となる。

【０１７７】従って、本実施形態に係るデジタルコンテンツ配布システムによれば、付加価値の高いデジタルコンテンツを、安全に半導体記憶媒体やデジタルネットワーク上で流通させることが可能となり、デジタルコンテンツ配布サービスなどへの応用が可能となる。

【０１７８】なお、デジタルコンテンツの保護においては、配布経路暗号化動作および出力経路暗号化動作のうちのいずれか一方を用いたシステムとしてもよいし、また、両者を組み合わせ、２つの独立した暗号方式によって、デジタルコンテンツの保護を行うシステムとしてもよい。

【０１７９】

【発明の効果】以上説明したように、本発明によれば、デジタルコンテンツの著作権を保護しつつ、ユーザの視聴覚欲求を刺激することの可能な、デジタルコンテンツの最終出力が可能となる。

【図面の簡単な説明】

【図１】本実施形態に係るデジタルコンテンツ配布システムの概略構成図。

【図２】本実施形態に係るデジタルコンテンツ配布システムの概略動作フローチャート。

【図３】本実施形態に係る情報処理装置の概略構成図。

【図４】本実施形態に係る情報処理装置の概略構成図。

【図５】デジタルコンテンツ配布装置から配布されるデジタルコンテンツの暗号化方法の一例を示す説明図。

【図６】図５に示す暗号化方法で暗号化されたデジタルコンテンツを表示装置で表示した場合の表示イメージを

【図８】本実施形態に係る表示制御装置の概略構成図。

【図９】本実施形態に係る表示装置の概略構成図。

【図１０】本実施形態に係る表示装置の概略構成図。

【図１１】表示制御装置から出力される表示データの暗号化方法の一例を示す説明図。

【図１２】表示制御装置から出力される表示データの暗号化方法の一例を示す説明図。

【図１３】本実施形態に係る情報処理装置の概略構成図。

【図１４】図１３に示した情報処理装置の概略動作を示す説明図。

【符号の説明】

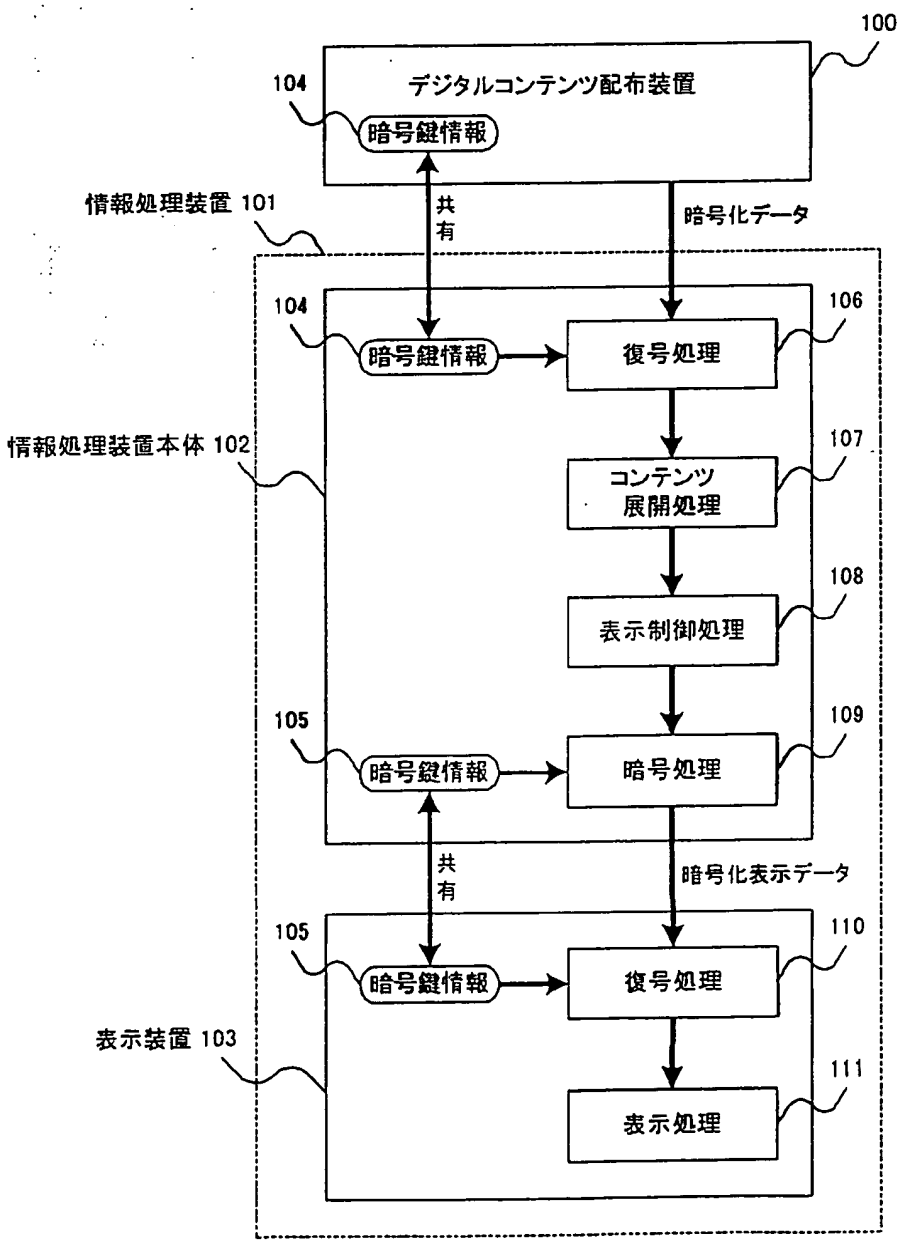
１００：デジタルコンテンツ配布装置
１０１：情報処理装置
１０２：情報処理装置本体
１０３：表示装置
１０４：暗号鍵情報
１０５：暗号鍵情報
１０６：復号処理
１０７：コンテンツ展開処理
１０８：表示制御処理
１０９：暗号処理
１１０：復号処理
１１１：表示処理
３０１：中央演算装置（ＣＰＵ：Central Processing Unit）
３０２：システムメモリ
３０３：表示制御装置
３０４：表示メモリ
３０５：入力制御装置
３０６：通信制御装置
３０７：バス
３０８：復号処理部
３０９：コンテンツ展開処理部
４０１：暗号処理部
４０２：復号処理部
４０３：データドライバ
７０１：不揮発性記憶装置
８０１：メモリ制御部
８０２：タイミング生成部
８０３：タイミング信号
８０４：メモリ制御信号
８０５：メモリアドレス信号
８０６：ＬＣＤ（Liquid Crystal Display）制御部
８０７：ＬＣＤ制御信号
８０８：平文表示データ
８０９：タイミング制御部
８１０：ＬＣＤ表示データ

27　　28

８１３：暗号化Ｓ／Ｐ済ＬＣＤ表示データ
８１４：パラレル／シリアル変換回路（Ｐ／Ｓ回路）
８１５：暗号化ＬＣＤ表示データ
８１６：遅延回路
８１７：遅延済ＬＣＤ制御信号
９０１：ＣＬ２信号
９０２：暗号化表示データ
９０３：ＣＬ１信号
９０４：ＬＣＤ駆動用電源
９０５：液晶駆動出力信号
９０６：ラッチアドレスセレクタ
９０７：ラッチ回路－１
９０８：ラッチ回路－２
９０９：レベルシフタ
９１０：液晶駆動回路
９１１：ラッチ回路－３
９１２：平文表示データ
１００１：Ｓ／Ｐ回路
１００２：Ｐ／Ｓ回路
１００３：Ｓ／Ｐ済表示データ
１００４：平文表示データ

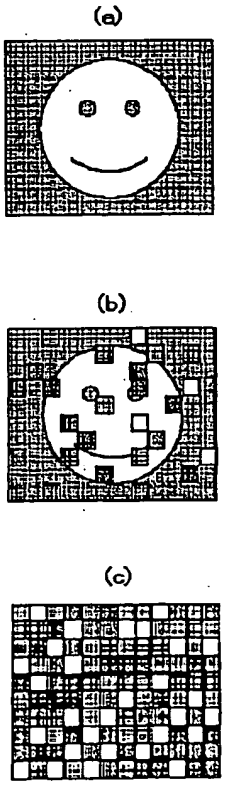
【図１】

図 1



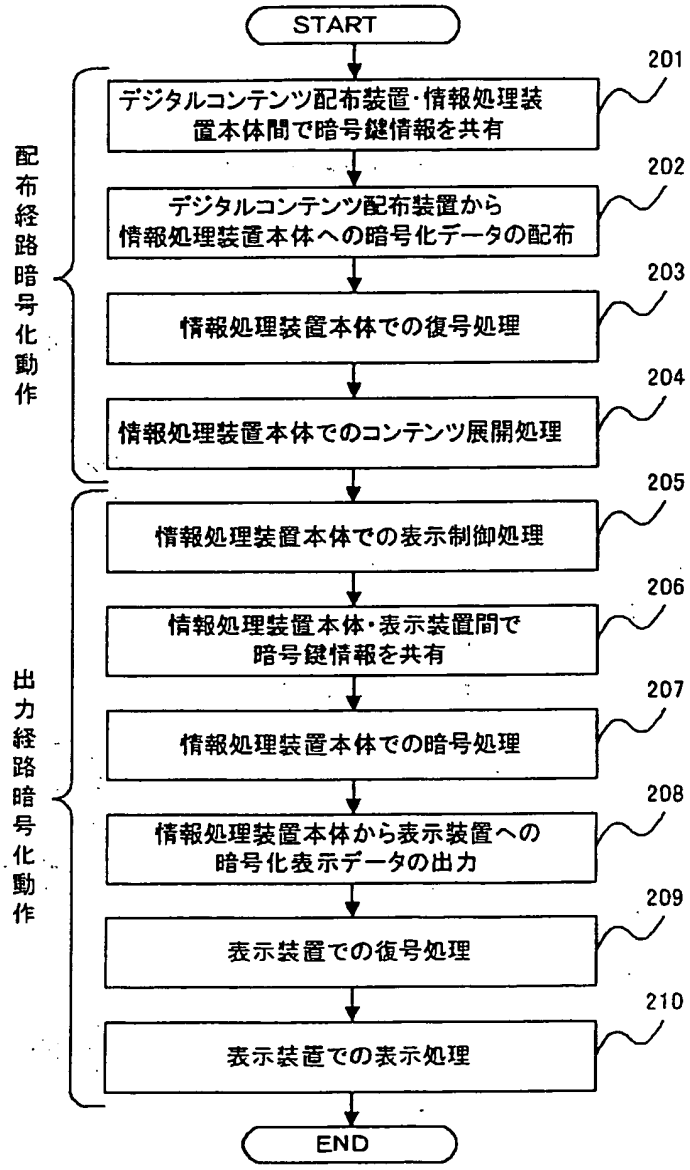

【図６】

図6



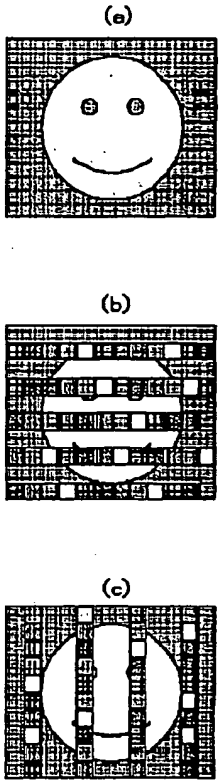
【図２】

図 2



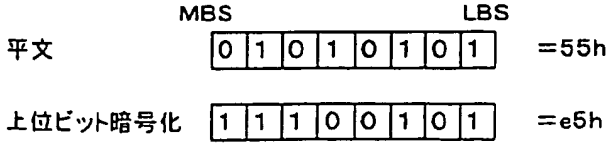

【図１１】

図11



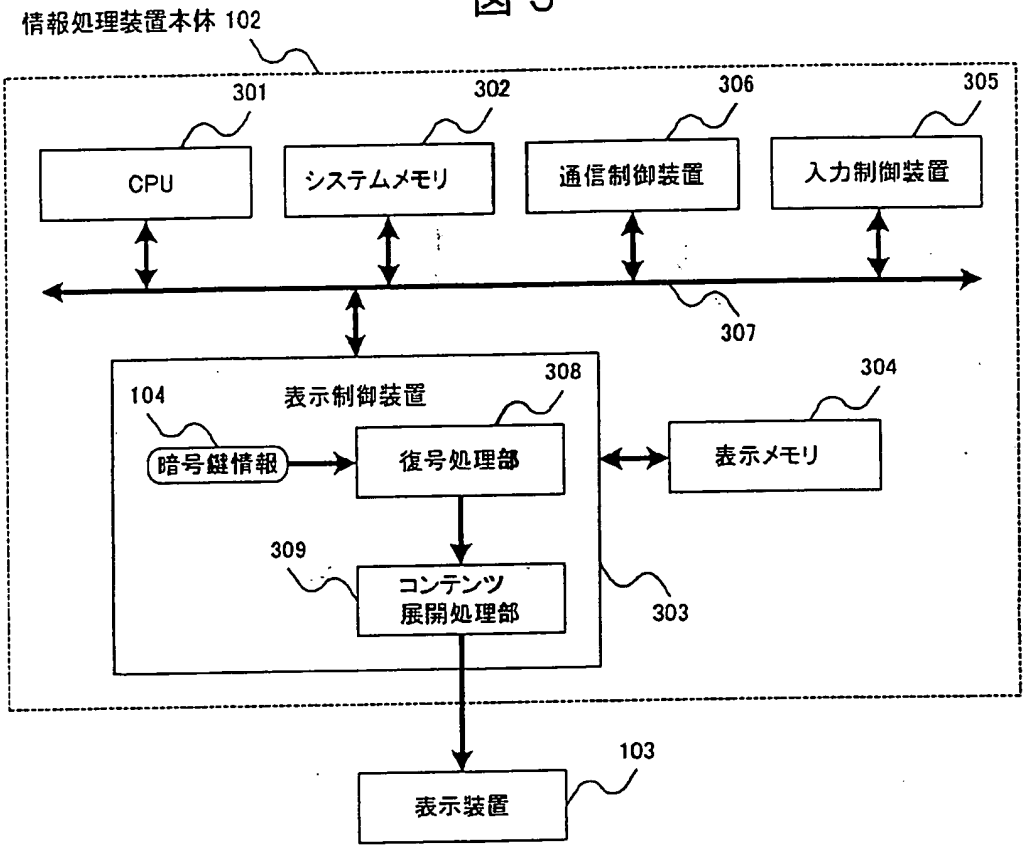

【図１２】

図 12



【図３】

図 3



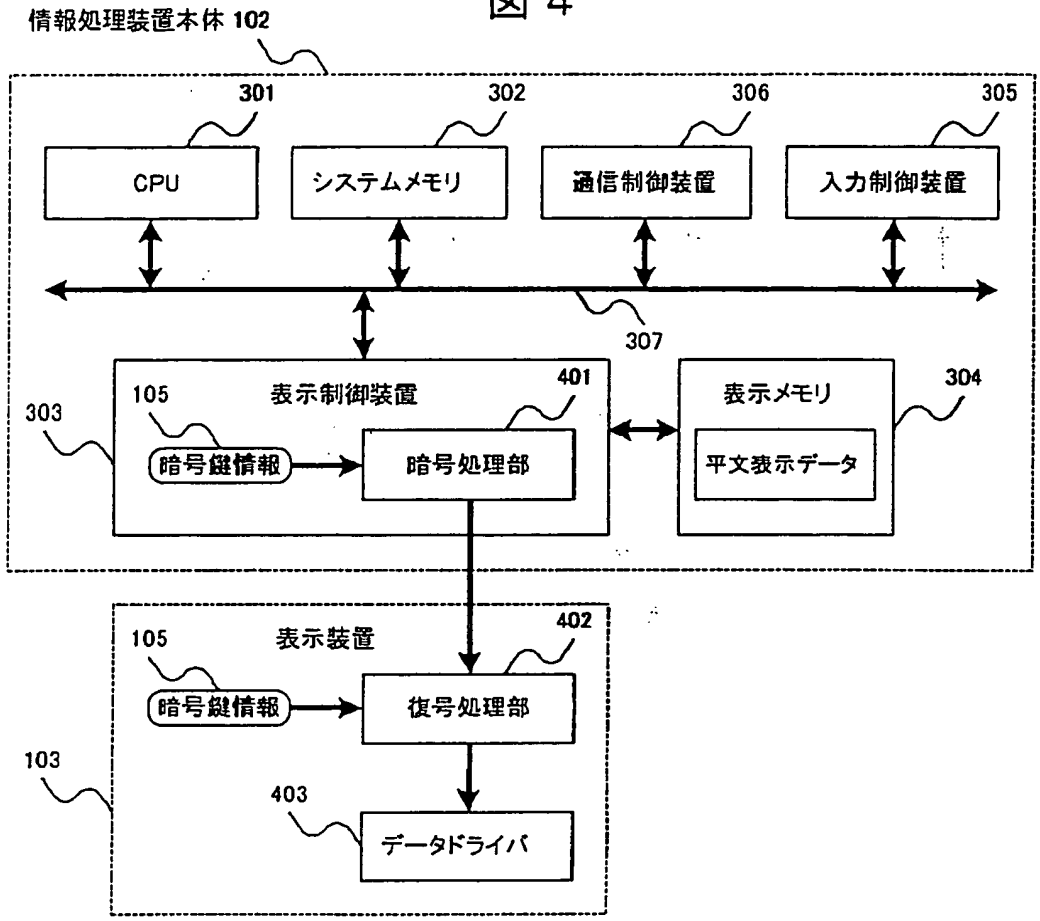

【図５】

図 5

| 暗号化対象 | 暗号鍵情報なしに得られるピクチャデータ | | | 符号割り当て量@ピクチャデータ | 暗号処理量@ピクチャデータ |
|---|---|---|---|---|---|
| | I | P | B | | |
| Iピクチャデータ | × | × | × | 大 | 大 |
| Pピクチャデータ | ○ | × | × | 中 | 中 |
| Bピクチャデータ | ○ | ○ | × | 小 | 小 |

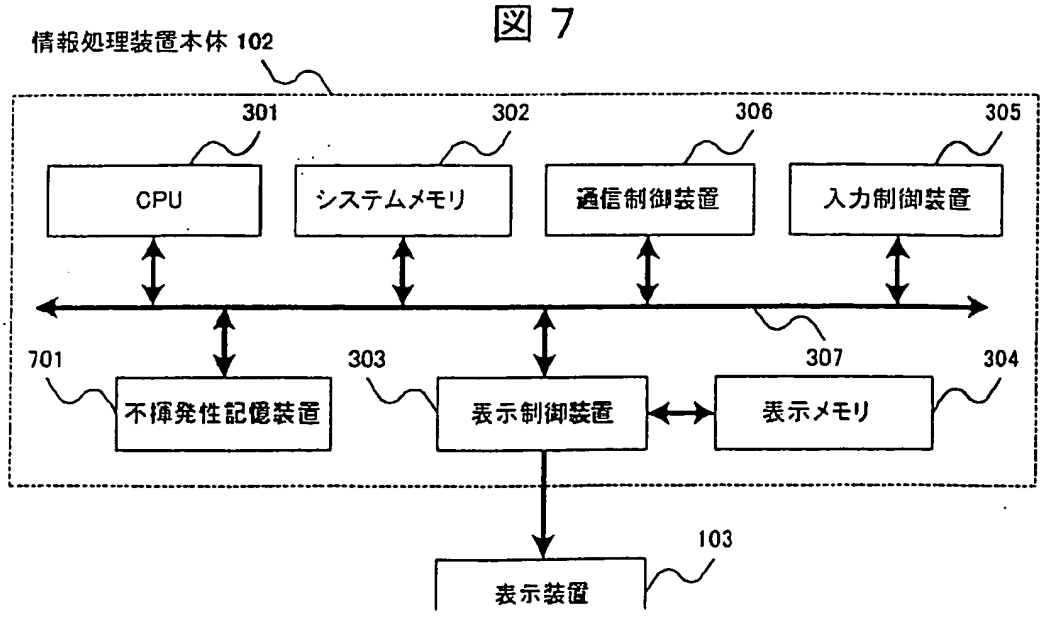
【図４】

図 4


情報処理装置本体 102
301
302
306
305
CPU
システムメモリ
通信制御装置
入力制御装置
307
303
105
表示制御装置
401
暗号鍵情報
暗号処理部
表示メモリ
304
平文表示データ
105
表示装置
402
暗号鍵情報
復号処理部
103
403
データドライバ

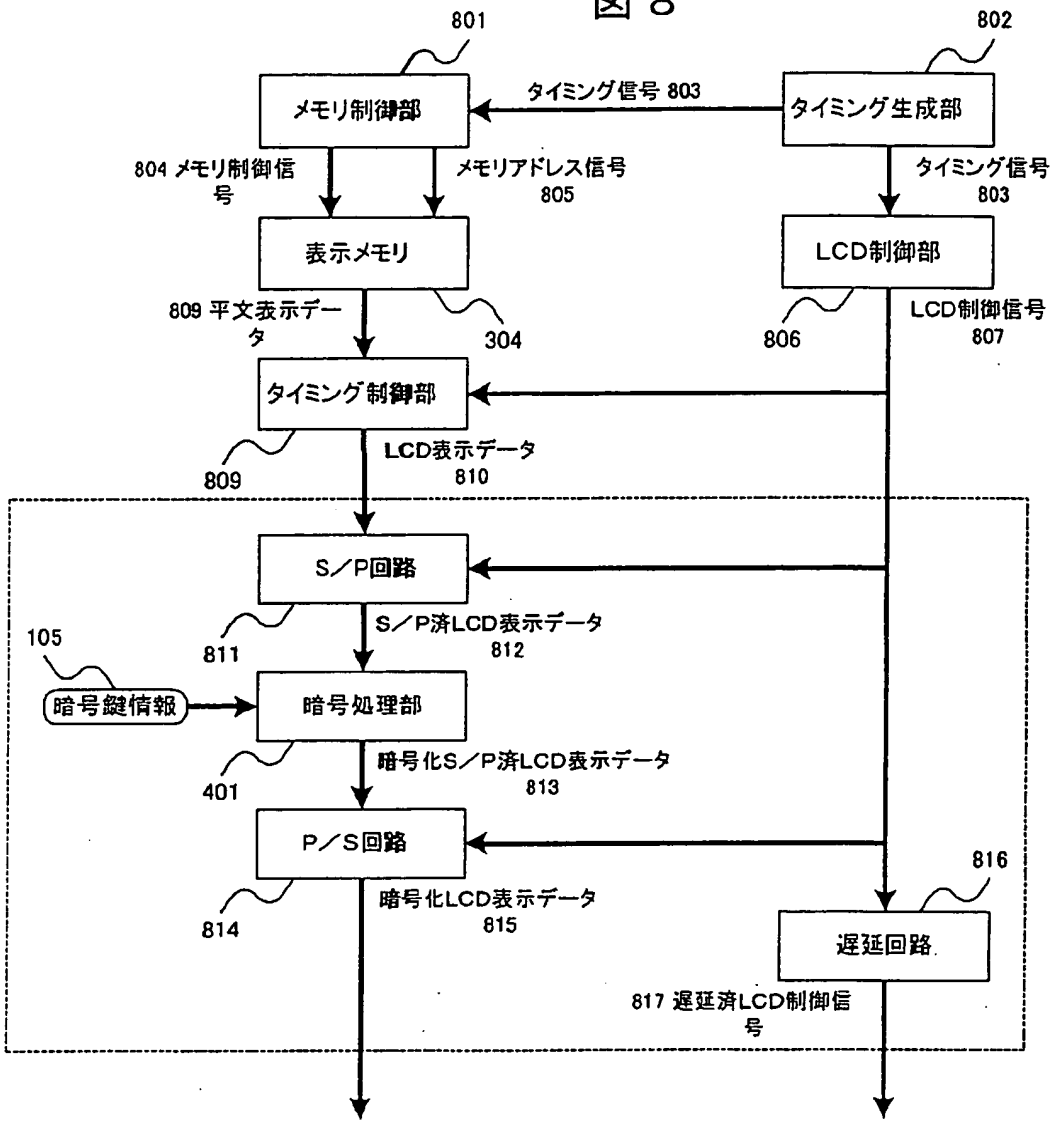
【図７】

図 7


情報処理装置本体 102
301
302
306
305
CPU
システムメモリ
通信制御装置
入力制御装置
307
701
303
304
不揮発性記憶装置
表示制御装置
表示メモリ
103
表示装置

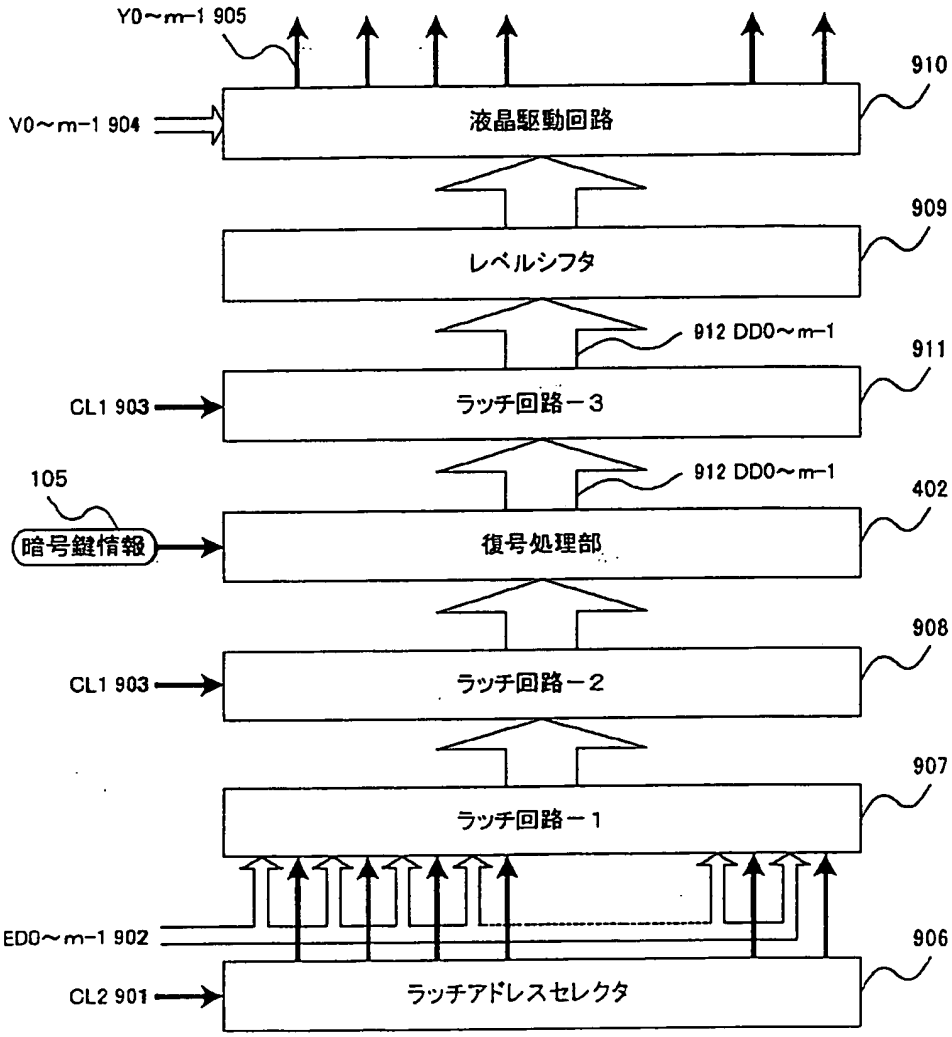
【図８】

図 8


801
802
メモリ制御部
タイミング信号 803
タイミング生成部
804 メモリ制御信号
メモリアドレス信号 805
タイミング信号 803
表示メモリ
LCD制御部
809 平文表示データ
304
806
LCD制御信号 807
タイミング制御部
809
LCD表示データ 810
S／P回路
811
S／P済LCD表示データ 812
105
暗号鍵情報
暗号処理部
401
暗号化S／P済LCD表示データ 813
P／S回路
814
暗号化LCD表示データ 815
816
遅延回路
817 遅延済LCD制御信号

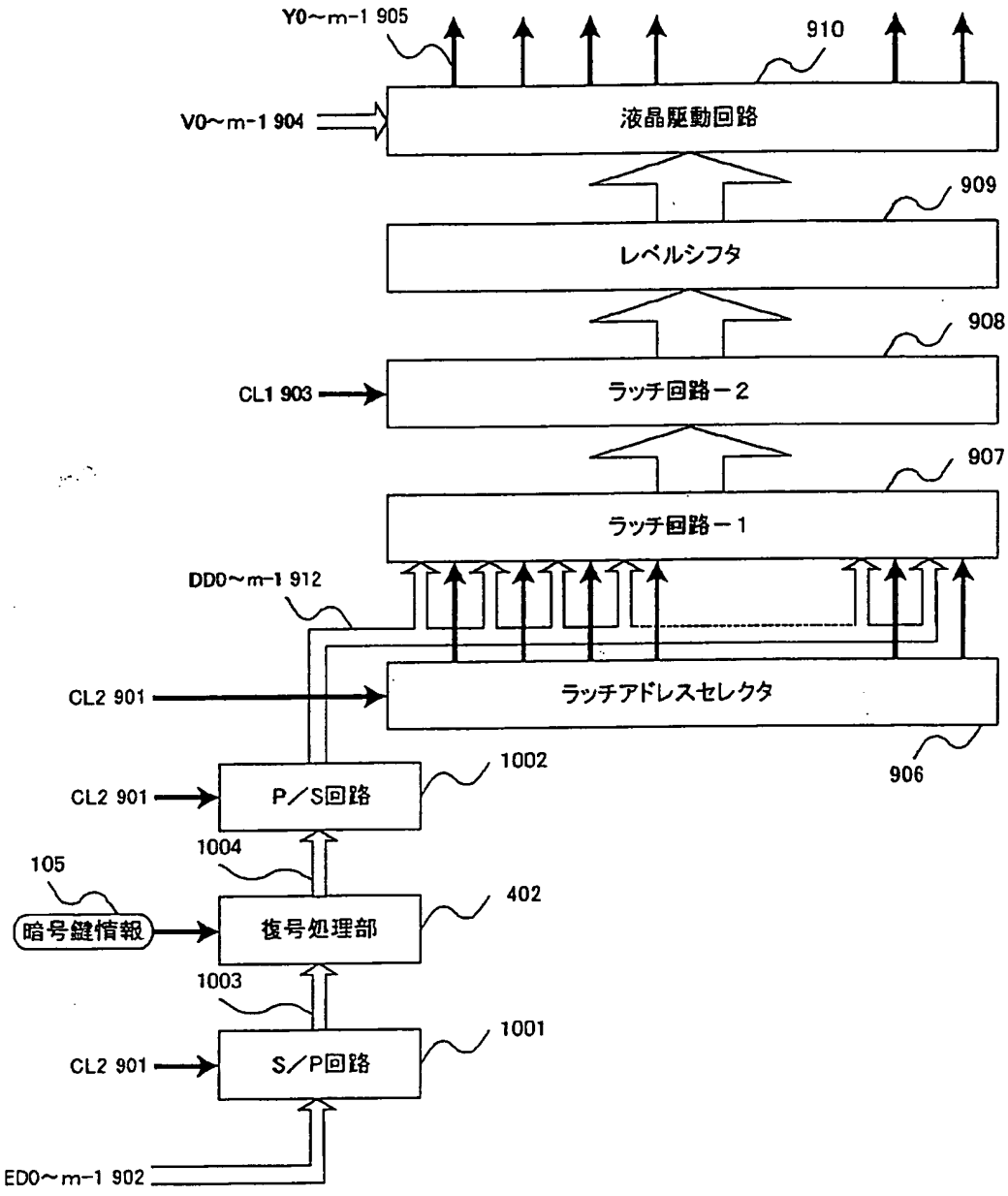
【図９】

図 9


Y0～m-1 905
910
液晶駆動回路
V0～m-1 904
909
レベルシフタ
912 DD0～m-1
911
CL1 903
ラッチ回路－３
105
暗号鍵情報
912 DD0～m-1
402
復号処理部
908
CL1 903
ラッチ回路－２
907
ラッチ回路－１
ED0～m-1 902
906
CL2 901
ラッチアドレスセレクタ

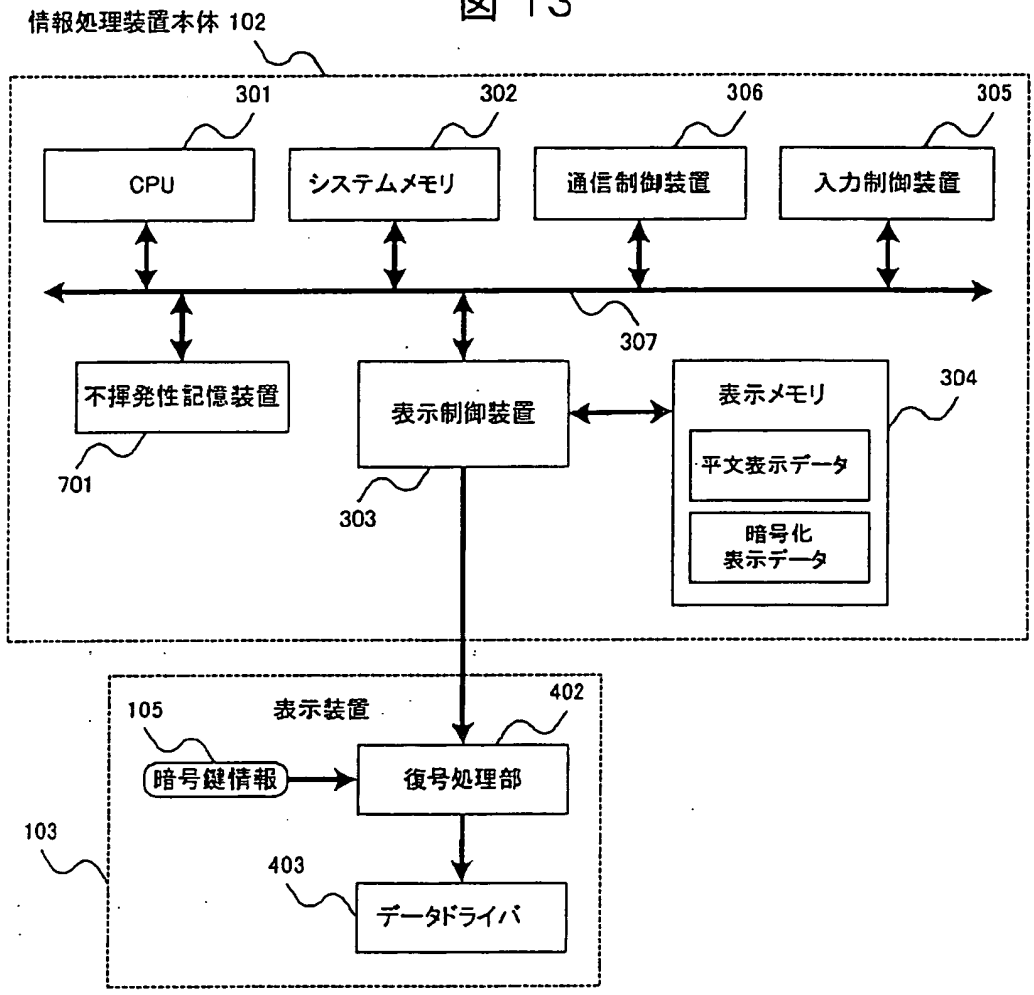
【図１０】

図 10


Y0～m-1 905
910
液晶駆動回路
V0～m-1 904
909
レベルシフタ
908
CL1 903
ラッチ回路－2
907
ラッチ回路－1
DD0～m-1 912
CL2 901
ラッチアドレスセレクタ
906
CL2 901
P／S回路
1002
1004
105
暗号鍵情報
複号処理部
402
1003
CL2 901
S／P回路
1001
ED0～m-1 902

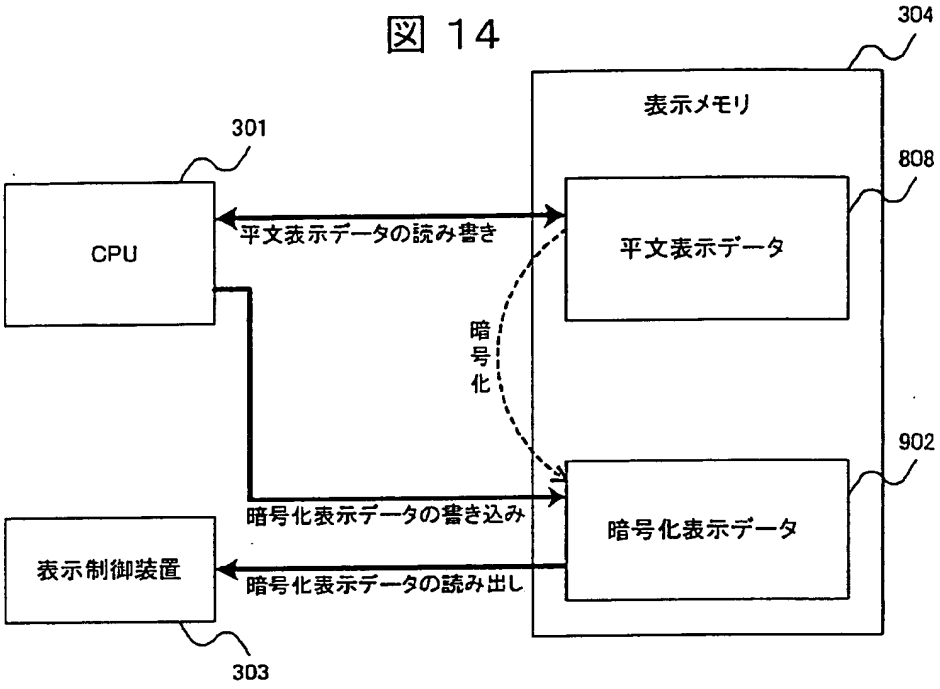
【図１３】

図 13


情報処理装置本体 102
301
302
306
305
CPU
システムメモリ
通信制御装置
入力制御装置
307
不揮発性記憶装置
701
表示制御装置
303
表示メモリ
304
平文表示データ
暗号化
表示データ
105
表示装置
402
暗号鍵情報
復号処理部
103
403
データドライバ

【図１４】

図 14




フロントページの続き

(72) 発明者　朝日　猛
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

Ｆターム(参考)　5C064 CA18
5J104 AA34 AA37 AA39 DA02 EA02 EA04 JA03 NA02